CONCEALBrowse™

Securing the Digital Edge: The Case for Browser-Centric Cybersecurity

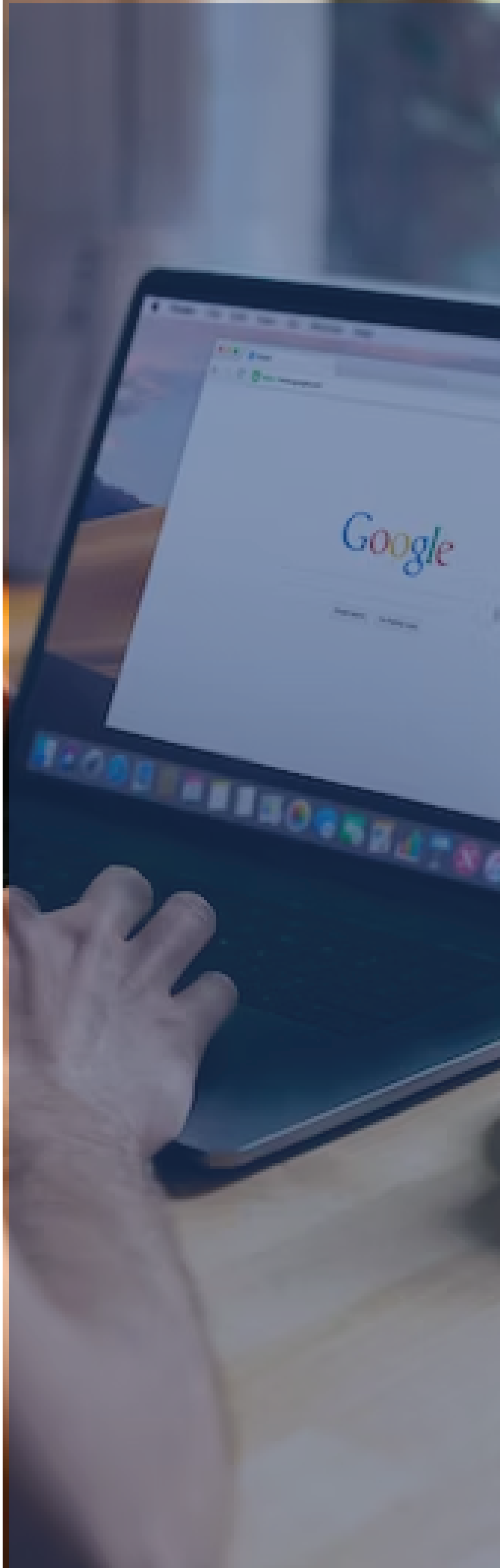
www.conceal.io

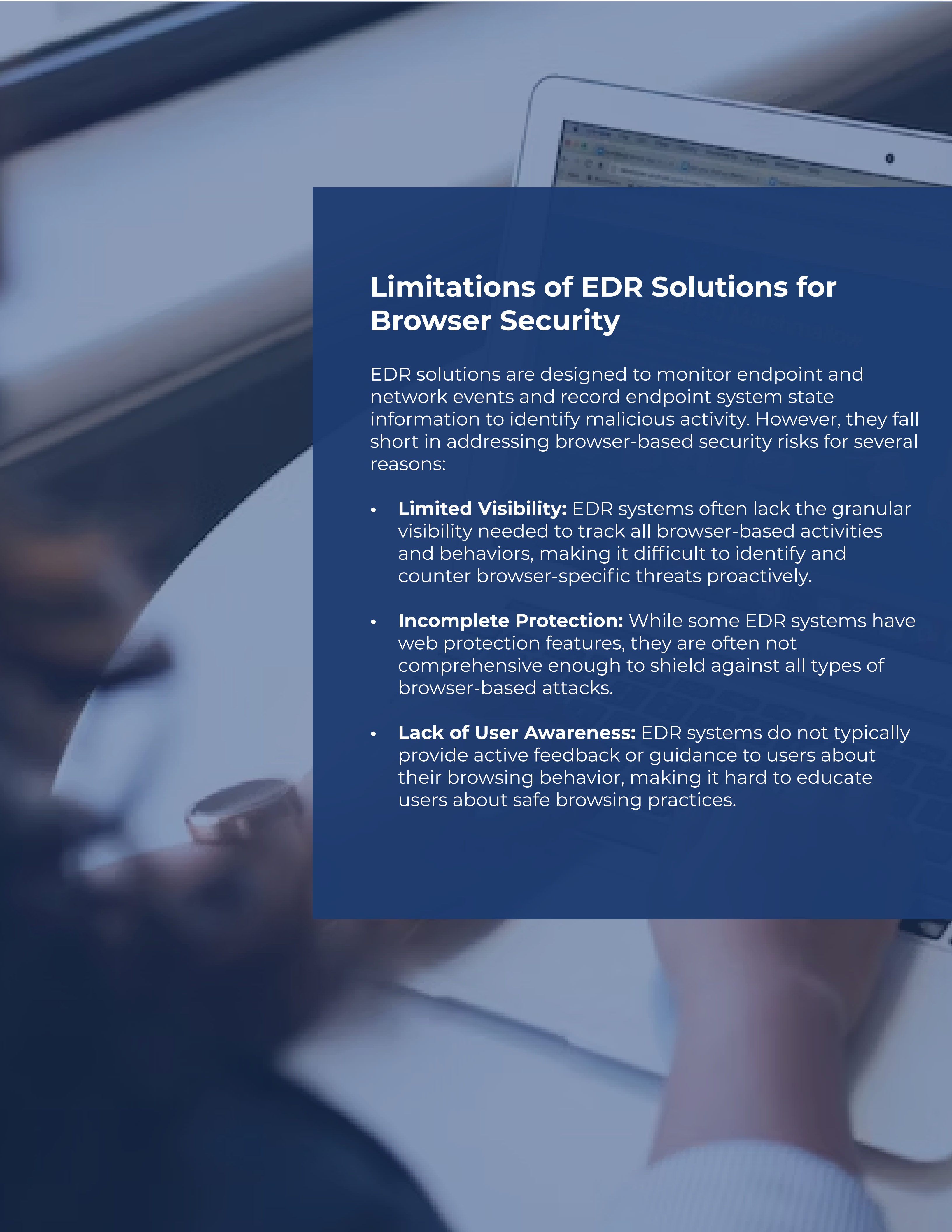
Introduction

Endpoint Detection and Response (EDR) systems have long been a mainstay of cybersecurity strategy, providing invaluable detection, response, and threat-hunting capabilities. However, as more work moves online and the web browser emerges as a new battleground for cybersecurity, the limitations of EDR solutions are becoming apparent. Rather than being seen as another point solution, ConcealBrowse enhances and complements EDR by integrating with leading EDR vendors. This whitepaper explores the shortcomings of EDR systems for managing web browser security and makes the case for implementing a specialized browser-centric cybersecurity solution alongside your EDR.

The Emerging Threat Landscape and the Role of the Browser

The cybersecurity landscape is constantly evolving, with threat actors adopting increasingly sophisticated techniques. Today, much of the action is taking place in the web browser, where workers access a variety of cloud-based apps and services. From sophisticated phishing attacks to credential theft, the browser has become a prime target for cybercriminals. Yet, while EDR systems are adept at securing endpoints from device-focused attacks, they often fall short when it comes to securing web browsers.





Limitations of EDR Solutions for Browser Security

EDR solutions are designed to monitor endpoint and network events and record endpoint system state information to identify malicious activity. However, they fall short in addressing browser-based security risks for several reasons:

- **Limited Visibility:** EDR systems often lack the granular visibility needed to track all browser-based activities and behaviors, making it difficult to identify and counter browser-specific threats proactively.

- **Incomplete Protection:** While some EDR systems have web protection features, they are often not comprehensive enough to shield against all types of browser-based attacks.

- **Lack of User Awareness:** EDR systems do not typically provide active feedback or guidance to users about their browsing behavior, making it hard to educate users about safe browsing practices.

Why Rely Solely on Your EDR When You Can Stop Threats at the Browser

Depending on EDR alone for cybersecurity leaves your organization exposed to a myriad of browser-based threats that EDR solutions may not be equipped to handle. By implementing a browser-centric solution like ConcealBrowse, you can prevent these threats at their source - the browser.

The Case for a Browser-Centric Cybersecurity Solution

To address the unique complexities and security risks of the web browser, organizations need a browser-centric cybersecurity solution that complements their existing EDR.

- **Comprehensive Protection:** A browser-centric solution like ConcealBrowse is designed to address the full range of browser-based threats, offering robust protection against phishing, credential theft, ransomware, and more.

- **Enhanced Visibility:** With a solution like ConcealBrowse, organizations gain a granular view of browser activity, enabling them to detect and address threats more effectively.

- **User Education:** Browser-centric solutions can provide real-time feedback to users about their browsing behavior, promoting safer browsing practices.

The Power of Complementary Protection

While a browser-centric solution offers comprehensive protection against web-based threats, it does not negate the need for EDR. Instead, the two solutions should be viewed as complementary, each addressing different aspects of an organization's cybersecurity needs.

EDR systems remain critical for monitoring endpoints, identifying and remediating threats, and providing in-depth incident analysis. Meanwhile, a browser-centric solution like ConcealBrowse adds an essential layer of protection to prevent browser-based threats that EDR systems might miss. Together, these solutions provide a more robust and comprehensive approach to cybersecurity.

How ConcealBrowse Complements EDR

While EDR solutions are valuable for general endpoint protection, they may fall short when dealing specifically with web browser security, as explored above. It is crucial to pair them with a dedicated browser security solution like ConcealBrowse to protect the organization's edge effectively. The two technologies complement each other to provide a comprehensive security solution:

Not Specialized for Browsers - EDR solutions, while robust for endpoint threats, are not specialized for the complexities and potential threats that emerge within web browsers. They can fall short in detecting and responding to web-specific threats like malicious or obfuscated URLs. Conceal's core mission is specifically to detect and proactively address web-based threats.

Limited Coverage for Web-based Attacks- While EDR solutions might prevent malware or ransomware at the device level, they may not adequately cover all forms of web-based attacks. ConcealBrowse is built to specifically defend against phishing, malvertising, or attacks launched from social media and other platforms where employees increasingly engage.

Challenging to Detect Zero-Day Browser Exploits - EDR solutions may not be equipped to detect zero-day browser exploits, whereas a dedicated browser security solution, like ConcealBrowse, has a focus on predicting and mitigating such vulnerabilities.

Unable to Address Unknown Web Threats - Traditional EDRs are often limited to known threat databases and can struggle with unknown or emerging threats on the web. In contrast, ConcealBrowse addresses unknown risks by isolating unknown activity in remote browser isolation.

Potentially Miss Browser Vulnerabilities - EDR solutions primarily focus on system-wide vulnerabilities and may potentially miss or under prioritize unpatched vulnerabilities within the browser. With a complimenting web-browser security solution, such as ConcealBrowse, this potential gap is addressed.

Limited Isolation Capabilities - Most EDR solutions do not have built-in isolation capabilities for web-based threats. ConcealBrowse's dynamic browser isolation is more effective as it sends risky URLs to isolation before they have the opportunity to affect the user's environment.

Inadequate Privacy Features for Web Browsing - EDR solutions might not provide the necessary privacy features for web browsing. A specialized web security solution, like ConcealBrowse, ensures that administrators only have access to necessary information, thus enhancing privacy.

Less Effective Policy Enforcement for Web Browsing - Policy enforcement on web browsing may not be as effective in traditional EDR solutions compared to specialized web browser security solutions, which can integrate with existing policy controls for more effective administration.

Conclusion

As the web browser becomes a primary interface for work and a key target for cybercriminals, securing it requires a specialized approach. While EDR systems play a crucial role in overall cybersecurity, they cannot address all browser-related risks. A browser-centric solution like ConcealBrowse fills this gap, providing comprehensive, targeted protection for the browser. Together, EDR and browser-centric solutions can deliver robust, layered cybersecurity, helping organizations secure the digital edge in an increasingly complex threat landscape.

About Conceal

Conceal is a fast-growing cybersecurity company that offers innovative technology solutions to our customers, globally. Each team member reflects our company's main goal: to protect the world from ever-growing cybercrimes.

Conceal enables organizations to protect users from malware and ransomware at the edge. The Conceal Platform uses Zero Trust isolation technology to defend against sophisticated cyber threats. Conceal is used by organizations of all sizes globally to ensure their users and IT operations remain secure, anonymous and isolated from attacks.

Disguise and protect your enterprise's online presence.

706-481-2642 | conceal.io | info@conceal.io

CONCEAL